Trust and Compliance Management Models in Emerging Outsourcing Environments

Aljosa Pasic, Juan Bareño, Beatriz Gallego-Nicasio, Rubén Torres, Daniel Fernandez

To cite this version:

Aljosa Pasic, Juan Bareño, Beatriz Gallego-Nicasio, Rubén Torres, Daniel Fernandez. Trust and Compliance Management Models in Emerging Outsourcing Environments. 10th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society (I3E), Nov 2010, Buenos Aires, Argentina. pp.237-248, 10.1007/978-3-642-16283-1_27 . hal-01055011

HAL Id: hal-01055011

https://inria.hal.science/hal-01055011

Submitted on 11 Aug 2014

Trust and Compliance Management Models in Emerging Outsourcing Environments

Aljosa PASIC, Juan BAREÑO, Beatriz GALLEGO-NICASIO, Rubén TORRES,
Daniel FERNANDEZ
Atos Origin sae, Albarracin 25, Madrid, 28037, Spain
Tel: +34 91 2148663, Fax: + 34 91 7543252, Email: aljosa.pasic@atosorigin.com

Abstract. Businesses today have more than ever a sharp focus on reducing capital and operational expenses. Business Process Outsourcing (BPO), Knowledge Process Outsourcing (KPO) and adoption of shared service models have all increased on a global scale. This results in an emerging complexity and volatility of business relationships. As the future internet of services evolves towards dynamic "service marketplaces", where shared services are discovered, negotiated and choreographed at run-time, the new approaches to the compliance management in complex environments are needed. We argue that one of the key issues to address is trust. This paper describes the compliance management models in emerging outsourcing environments that include use of shared services such as cloud computing services. In this context, we briefly present MASTER project that, among other things, integrates several mechanisms to increase the trust levels among stakeholders. Finally, we present a solution for the automated evidence collection at the service provider site and discuss related trust issues.

Keywords: Compliance, Internal Control, Trust, Cost Reduction, Outsourcing

1 Introduction

Businesses today have more than ever a sharp focus on reducing capital and operational expenses. Market push and cost saving is driving the convergence of different sources of value in souring options: outsourcing specialized in knowledge or resources are now being mixed with those specialised in convenience and scale.

The advent of cloud service providers, for example, may now allow specialized business process outsourcing (BPO) providers to focus on knowledge and still provide compelling scale in the infrastructure by using shared services online. In a "classic" business process outsourcing context the outsourcing partner not only takes over the ICT but also takes responsibility for the compliance related tasks such as evidence collection. Business Process (BP) execution is assisted by often software tools that should be able to collect compliance-specific evidence and to generate respective execution events. Although business process outsourcing involves a re-allocation of responsibility for performing all or part of a business process, the regulatory compliance responsibility and obligations remains with the process owner, which puts a lot of emphasis on trust relationships.

In this paper we start with an analysis of emerging trends and shifts in outsourcing models and partner relationships. Then we cover compliance management (CM) in general and CM in specific outsourcing contexts where a change in trust relationship is directly related to reallocation of evidence collection responsibility.

Implementing business process compliance requires means of compliance engineering, control tasks, assessment etc as well as some level of automation for some of these tasks. Full or partial automation of CM tasks is another trend covered in this paper and we will present how our approach, developed in MASTER project [1], facilitates CM task automation and flexibility. MASTER project is a collaborative project funded under the EU 7th Research Framework Programme and is currently developing a framework that will help, in particular, to reduce the compliance risk in externalization scenarios and will ensure an effective control as if business processes were running in a trusted administrative domain. Finally, this paper concludes with the trust assessment for different CM models and outsourcing settings.

2 Trends and Shifts in Outsourcing

Sourcing is a wide concept that entails various approaches. The choices range from insourcing, i.e. in-house operations, to complete outsourcing. Information Technology (IT) Outsourcing, for example, suggest externalisation of variety of IT services, ranging from Data Entry Jobs, through Software Development to Website Designing. While various kinds of partial outsourcing options as well as joinsourcing options exist, another approach, derived from the evolution of IT services markets is emerging. Traditional low value human resource-driven (HRD) outsourcing e.g. call centre, desktop and helpdesk support or maintenance of mainframe computers are now complemented by shared service based (SSB) IT services market such as on-demand or cloud computing. The value shift is towards scale, usability etc. In parallel, existing Expertise and knowledge-driven (EKD) outsourcing, such as legal assistance or third party assessments (TPA), is becoming the mainstream trend in the IT markets.

For a long time, IT outsourcing has been perceived as a technology issue, but actually it has less to do with technology than with the business itself or its costs. The existence of different outsourcing models and possibilities is therefore stimulated by cost analysis as much or even more than capabilities or value proposition of service provider. Historical experience says that company can save a minimum of 20% reduction in costs [2] by outsourcing. We argue that, besides cost and the additional value for the business, trust relationships are going to play an increasingly important role in this analysis of outsourcing options and we will illustrate this with examples considered in MASTER project. In principle, trust is already considered in some outsourcing approaches. In joinsourcing (co-sourcing), for example, a customer and its IT providers form an alliance in which operations are not fully outsourced and the customer keeps IT under its own control. Service level and value agreements are common in this form of outsourcing, but the main advantage for customer is close monitoring of these agreements and increased perception of trust. Another form of sourcing is the solution partnership that typically supports a specialised business line or product. Centre of excellence [4] idea was presented in 2004 with several advantages within the "hybrid" or "global sourcing" frameworks. Atos Origin, the second largest BPO provider in Western Europe [3], launched another outsourcing model in 2009, so called “agile outsourcing” that spans over three lines of our business: Managed Operations, Infrastructure Solutions (including utility services) and Application Management.

The most dynamic outsourcing model, however, is yet to come. It should combine many of the above mentioned elements, including transformation partnership or expertise and knowledge-driven (EKD) services as well as ad-hoc composition of shared services for ICT support. For this theoretic model, that will be enabled by the existence of “dynamic service markets” in the future internet, hybrid value proposition and relationship driven coalitions will be the main drivers. We introduce term “combo-sourcing” to refer to this model. Service Oriented Architectures (SOA) provides a common platform that allows integrating services and components across organisational domains, reusing them in different business settings, and building applications through orchestrating services following the business needs. SOA not only allows the IT infrastructure to keep pace with the increased complexity and scale of modern business networks, but its flexibility and adaptability turns out to be a necessary precondition to execute business within these networks. These architectures, however, are characterized by an inherently distributed security administration and a number of unsolved security issues [5]. The move towards services also increases the emphasis on relationships, negotiations, and agreements. This brings particular challenges for the area management and measurement of security. Rather than being predefined and fixed over long periods of time, as in conventional computing, the architecture of shared service is defined in terms of the requirements specified for the service functionality and the discovery, selection, choreography or adaptation processes applied across all relevant services. These processes, hence the architecture, may also be governed by models, patterns, and policies. We argue that in the current state of the art, issues such as compliance may limit ad-hoc changes in service compositions compliance while patterns may constrain entire architectures that have been proven to work well in specific contexts.

3 Compliance Management

Compliance is a term generally used to refer to the conformance to a set of laws, regulations, policies, or best practices. While compliance is a final goal, process designed to help the organization accomplish it is called internal control process [6]. As a matter of fact, compliance or business objective setting is a precondition to implement an internal control framework. Compliance management, as defined in [7] is the term referring to the definition of means to avoid policy violations where policies are derived from compliance requirements. Compliance management (CM) also refers to standards, frameworks, and software used to ensure the monitoring and control of this policy enforcement.

Compliance Management consists of many tasks roughly grouped around three main phases:

- Compliance engineering: Compliance engineering consist in the translation of non-trivial regulatory compliance requirements, business goals or organizational policy aspects, that are often expressed in natural language, into technical controls that can be deployed in operational infrastructure and can generate evidences which, at a later stage, enables compliance risk assessment and eventual audit certification. Set of operation policies is used as an interface to operational compliance infrastructure and internal control process.
- Operational compliance infrastructure: indicators that are tailored to measure levels of compliance are used in combination with software components and different types of internal controls that enable evidence collection as well as some kind of corrective/compensating actions. Parts of this infrastructure include signaling, monitoring and enforcement components.
- Assessment of compliance: in ideal situation, companies should have ability to continuously assess compliance levels not only for processes running on ICT systems at their premises, but also for those processes that run on external IT systems. Evidence aggregation, correlation, analysis, control refinement, risk re-assessment, etc., are some of tasks related to this phase of compliance management. Internal audits, sometimes called first party audits, are conducted by, or on behalf of, the organization itself for internal purposes. The internal or external auditors assess whether the controls are properly designed, implemented and working effectively, and make recommendations on how to improve internal control

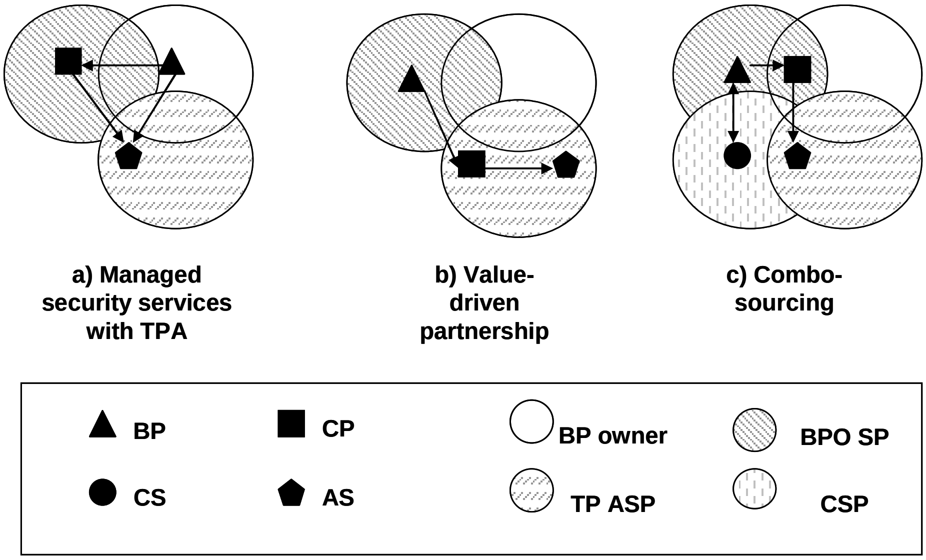
Currently, compliance management is relying heavily on manual, error-prone, sample-based procedures undertaken by either internal or external auditors. Automation can be achieved by means of software tools [8], although there is still a way to go. Many software vendors moved to Governance, Risk and Compliance (GRC) market with previously existing tools and without sound CM framework that could actually remediate governance gaps which are especially relevant in outsourcing environments. Choice of security controls, for example, which is often based on static risk assessment driven by regulatory compliance requirements, is a typical top-down process which is not sufficient to assure compliance in environments with complex governance such as outsourcing environment. Actually, there are a multitude of reasons for which deviations from an expected business process might happen (e.g., human factors, service downtimes). The accuracy and coverage of these security controls could be increased through automated evidence collection, tools that provide feedback based on operational indicators or tools such as event correlation analysis. However, the information from these tools used in compliance management detection and assessment phase should be used not only for upper level reporting, but also for real time corrective actions. In addition, this information could be used to improve trust management (e.g. through event tagging, reputation mechanisms etc) in complex outsourcing environments. MASTER framework for integrated compliance management is one of the first attempts to provide coherent coverage of these issues.

4 Modeling Compliance Management in MASTER

In the emerging outsourcing environment, the BPO or service provider may not be able to offer all the required information or compliance evidences to the customer, the business process owner. Customers might believe that events or related evidences provided by service providers are not authentic. Service provider may not want to reveal all contents of events emitted by the outsourced business process or shared services, since this may expose sensitive information about the service provider unnecessarily. In addition, customers can constrain information flow of sensitive information or can impose security objectives for each type of data. Consequently, the whole trust framework for Compliance Management requires some re-assessment for these environments with multiple trust levels (we will use shorter term multi-trust environment).

One possibility in the complex outsourcing scenario is to move the responsibility for the fulfilment of the control objective to the outsourcing-provider together with the outsourced business process. To establish an agreement between parties, key assurance indicator (KAI) can be used. The basic idea behind the indicators originally introduced in [22] is that they give a meaningful evaluation of compliance of the process (Key Assurance Indicator, KAI) and measure how well the control process is implemented (Key Security Indicators, KSIs). More formally speaking, KAI defines how good is the process P is with respect to the ideal process P (ideal), e.g. if all the traces of this process are 100% compliant. Alternatively, service provider might expose the controls in place which implement the required control objective (KSI in this case). The intuitive meaning of Key Security Indicator for Correct Operation of Controls (KSIcorrect) is that it defines how good is a given control process (CP) applied to business process (BP) with respect to CPideal applied to BP. In the KSIcorrect definition we also use an evaluation function that compares a result of applying CP to BP and result of CP(BP) that is also produced by CPideal(BP). Intuitively speaking, in this way we define how good is the CP with respect to CPideal for our BP. Another indicator is Key Security Indicator for Control Coverage that, for a given observation period O and evaluation function Eval, defines the coverage of our BP by the given CP (full definitions can be found in [22]).

The advantage of approach that uses KSI is that the providers can make their own choice on how to implement the control (as long as it is complies with the abstract specification of the control process or as long as it guarantees satisfaction of the outsourced control objective) and thus keep the control over the business process. However, the service provider might not be able to implement the specified control process or might not want to be responsible for the violation of the control objective. In this case the implementation of the control objective and responsibility for its fulfilment is kept external from the party which implements business process Thus, the service provider doesn’t have to worry about the enforcement of the control objective, but must provide sufficient visibility and control to the party responsible for the control objective fulfilment to enable monitoring and enforcement of this control objective. The advantage of this approach is that the providers do not have to implement any controls and thus the provider selection is more flexible (assuming enough evidence and control are provided). However, service providers might not want any external influence on their business processes due to the possibility of violation their internal regulations, and might not want to provide information the process uses internally due to the information disclosure. Thus, the outsourcing-client (or service requester) and outsourcing-provider (or service provider) need to agree on how much control and visibility are provided on the one hand and how much responsibility the provider holds on the other hand. The challenge in this case is an appropriate disaggregation of the control objective and the corresponding control process (implementation of the control objective) – parts of it will be ensured on the provider side and other parts on the requester side. In case where parts of the control objective are outsourced, they specify high-level requirements the provider must fulfil (outsourcing on the specification level, defining "what" must hold). In case control process fragments are outsourced, they define abstract operational semantic the provider must comply to (outsourcing on the implementation level, specify "how" to do it). To enable outsourcing on the specification and implementation levels, service providers must describe available functionalities to execute outsourced parts, such as monitoring and enforcement capabilities.



a) Managed security services with TPA

b) Value-driven partnership

c) Combo-sourcing

Fig. 1: Illustration of different outsourcing settings and flows for CM

In practice, control processes and a CM component placement is constrained by organizational governance models as well as a mapping between equivalent or complementary aspects of organisations that are involved in trust-driven exchange of information. The following roles are defined:

- Customer (owner of business process)
- Service providers (SP), here regarded as business process outsourcer (BPO) and Cloud Service Providers (CSP) that offer consumption and delivery model for shared IT services
- Third-party (TP) that offers services, such as assessment or auditing. Both SP and customer might want to use these third-party services (ASP is Audit Service Provider)

Compliance related events could be later automatically delivered either to the customer or to the TP that has compliance assessment knowledge and capabilities, as well as necessary event correlation or intelligence tools. Automated evidence gathering for compliance purpose, however, becomes a significant challenge in the case of processes outsourced to the BPO that also uses another outsourcer or CSP services such as storage or computing. An additional challenge is when service running at CSP is shared by several customers and CSP can not provide segregation of events so that the right information goes to the right customer. The following figure presents a number of combinations between business process (BP), control process (CP) and cloud services (CS). All of these might be requested to provide events or evidences to the TP services such as assessment services (AS) or external auditors. As we will see, the operational effectiveness of these controls depends strongly on trust between these stakeholders.

In all depicted settings there should be an agreement, corresponding to each data flow that spans two different "trust zones" and that includes constraints from both points of view. MASTER assumes the existence of a shared vocabulary between organisations (possibly negotiated offline), which is then used to label organisations, processes, and data. Once this labeling is in place, policies such as "don't send data labelled X to organisations labelled Y" can be stated.

Another situation occurs when the service provider may not be able to offer all the required evidences to the customer, such as the case of event generation at CSP. The typical public cloud service provider offers generic services (with some configuration options) to many clients. While each client requires being perfectly isolated from all other clients, the service provider has different ways of achieving this requirement. Basically, the service provider has to decide at which layer it wants to enforce the isolation. For example, if all applications share the same operating system, which may run on a massive compute cluster, multiple instances of MASTER can be deployed on the operating system so that each client application has its own MASTER instance and there is no chance that client accidentally sees events from other clients (see also [15] and [21]). However, operating system level controls may not be efficient as they can no longer be configured to meet the requirements of all clients. For instance, when a single application instance at CSP accommodates multiple clients, it becomes very difficult to tell which client generated the events.

5 Mechanisms to manage trust in MASTER

If we look at today’s TP audit services, wherein traditional audits are conducted for “after-the-fact” detection, often through manual checks by expensive consultants, we will see that implicit trust is already contemplated in this model. TP auditor usually physically visits the company and controls whether the company has correctly interpreted the existing regulations, whether control activities adequately covered the risks in the audit scope and have been correctly implemented, or whether business processes have been executed according to the policies. Although required interventions or authorisation are stipulated in contracts or depend on business affiliation, in practice there is always also a subjective component. Business relationships are based not only on business affiliation between parties, but also on the past history of working together, disposition toward each other’s expected behaviours, collaborative membership in common circles, and so on. Therefore, there are elements of business relationship that are uncertainty (the degree to which one party can predict the actions of another) and vulnerability (the level of consequence that occurs as a result of relating). The expectations of the behaviour of a party are also subject to change in time and the perception of the quality of the performance depends on these expectations. In this sense, trust level can also be seen as a local value based on local context and reputation.

Evaluation of trust mechanisms was done during the implementation of the first prototype for the financial sector scenario within the MASTER project. The prototype comprises two different parts: the simulation of the business flow and the conceptualization of the several entities which are part of the financial field. The evaluation contained trust-related information for all involved parties although it is focused on the architectural design and the software implementation taking into account the project's test-bed and the nature of the solution MASTER is intended to provide. The scenario involves users interested in the financial status of companies – ie. a bank that needs to decide whether to grant a loan. These users can initiate the simulation of the scenario by performing services such as a Debtor Identification followed by a Risk Classification Request. Identification of the debtor company is done by its tax code or name. In the latter case, it may result in a number of companies from which the user directly selects one. The debtor information is displayed to the user, which inputs the risk information –requested amount, payment deadline, etc. The external expert is queried for risk information about that particular debtor company following an automated decision tree. We evaluated several possibilities to increase trust, namely adjustable automation, delegation mechanisms and compensation actions.

Our conclusion was that the level of automation should be adjustable for the control of flow that goes back and forth between the human supervisor and the Control Infrastructure. This level may include also manual controls that could be monitored from the Control Cockpit. However, the input for manual controls would not be the event traces but would be from the human operator. The decision on automation level will depend both on component placement in outsourcing settings and trust between involved event producers and consumers. This means that we will likely have to add administrative delegation in the next prototype version. The trust level could be then increased by applying more complex monitoring rules, which execute additional checks on the middleware or even hardware event level. These rules take advantage of SOA and the possibility to decouple the components responsible for signaling and monitoring of events (evidence collection part of CM) and components responsible for correlation and assessment. SP can delegate access control to a third party with a higher reputation if this results in the overall trust level increase. The administrative delegation mechanism offers ways to apply fine grained distributed access control to monitoring and configuration rules in MASTER. Internal control process owner may delegate or specify who can have access to which MASTER infrastructure components.

6 Related work

A rather recent approach in CM is to provide some level of automation through automated detection. The majority of existing software solutions for compliance follows this approach. The proposed solutions hook into variety of event generating components and prepare data that supports auditing against hard-coded checks performed on the requisite system. These solutions often specialize in certain class of checks, for example the widely supported checks that relate to Segregation of Duty violations in role management systems. However, this approach still resides in the space of “after-the-fact” detection and there is limited applicability to outsourcing environments. In situations where complexity of the situation is conditioned by the presence of dynamically changing processes with services sometimes shared with other organisations, the complexity of compliance management requirements yields for a highly systematic and well grounded approach and we believe that MASTER is the right step in that direction.

There has been ongoing work on semantic compliance management, as shown in [11] and [12], where an approach for semantic compliance management for BPM is presented. However, the approach used concentrates on implementing internal controls based on static risk assessment. In a dynamic environment, such as the one that we address, risks are only partially known at the moment of compliance engineering.

Another approach is presented in [13] where the authors introduce the modelling of internal control objectives in business processes as a mean to integrate compliance requirements in business process design. Policies are meant to be more generic and do not depend on the previous definition of risks in processes. Like in our approach, policies are meant to be directly extracted from regulatory requirements which allows exchange of policies between stakeholders or discovering of policy conflicts.

There are also other approaches [14] that use deontic logic to model obligations and permissions, which can then be used in the design phase of a business process to verify the compliance of the process. There is also already a lot of work on trust and compliance, including trust calculi. In regard to CM business environment modelling, a related approach is for example Service Networks (SN), a graph-based approach to model a business environment as a set of business partners and their relations. The refinement from SNs to executable processes and software services has been motivated in [9] and first steps towards mapping of SNs to service choreographies are described in [10]. Similar to MASTER, the value calculations are based on a set of Key Performance Indicators (KPI) for measuring the performance of underlying business processes of the SN. The main difference, however, is that our focus is on Compliance Management and KPI are used to compare the compliant event traces (i.e., traces that have been made by running an ideal process) to all traces that have been made by a process within an observation period. Indicators are based on evidence, which in the context of MASTER is also provided by event traces. Therefore we can easily related policy violation to key performance indicators.

Clearly, trust management, contract management and autonomic security mechanisms are important aspects and these topics have been already extensively investigated. Trust management was firstly defined in [23] as "A component of security in network services. Trust management problem include formulating security policies and security credentials, determining whether particular sets of credentials satisfy the relevant policies and deferring trust to third parties". The pioneers of trust management have been tools such as PolicyMaker [24] and KeyNote [25]. Another very well known tool is Simple Public Key Infrastructure/Simple Distributed Security Infrastructure [26] that merged two previous approaches SPKI and SDSI, which combines binding names to public keys with authorization services. Few ideas of trust management are reflected in Cassandra [27], which is a role based trust management system ,Trust Policy Language (TPL) [28], and Query Certificate Manager (QCM) [29]. The topic of trust also incorporates issues such as trust establishment and trust negotiation. The existing research work and tools are exploiting different properties of trust, such as its relativity to a given context (not absolute), its directionality (from a relying party to a trusted party), its quantifiability, its existence and evolution in time and its transferability (potentially in absence of relational transitivity). Trust is modelled differently based on the reference application and nature of the established relationships between interacting entities. However, as we show in MASTER complex outsourcing scenarios, the challenge is to enable trust management with more modular that combined with distributed Compliance Management Infrastructure, could support the different phases and evolving models of outsourcing life-cycle.

7 Conclusions

As organizations are continuously exposed to an endless number of newly appearing and / or changing threats and as emerging outsourcing models affect its operation or the fulfillment of its objectives, the risk baseline is on a continuous shift. In addition, cost-driven changes in outsourcing settings, such as the use of shared services, might be in conflict with coherent compliance management and governance alignment. Here we have presented a compliance model framework that should fit a wide variety of needs as well as business models.

Compliance Management and related tools are attracting attention of both software vendors and customers that own business processes that are subject to regulatory compliance. An increasing number of organisations are moving towards the automated evidence data collection through deployment of tools while more advanced organisations use also automation of control checks and process (CCM/A, Continuous Control Monitoring or Auditing through tools such as GRC (governance, risk, compliance) software). This is obviously bringing many benefits, such as for example alignment of governance levels or executive dashboard implementation, where different risk or compliance views are presented to different governance levels. Although GRC tools can help management and internal auditors in the monitoring,and auditing of business processes, they will need to trust these tools,. Therefore, external auditors will first need to perform general computer controls reviews on these tools to get reasonable assurance that are operated and maintained securely. The other issues that influence dynamicity of trust in described environments include, for example, trust in inputs of monitoring tools (e.g. integrity of events produced at service provider or event traces aggregated by some software component) that have been monitored). In this paper we present approach based on adjustment of automated compliance evidence collection, flexibility in CM component placing, administrative delegation mechanisms and fine-grained compliance monitoring policies. These CM innovations would potentially bring changes in future business models that include third party assessment and external auditing.

References

1. http://www.master-fp7.eu/
2. Maximizing Business Potential Through Outsourcing, Atos Origin White Paper
3. Gartner „The Market trends: Business process outsourcing, Western Europe, 2003-2008“
4. Can you do more with less?, Atos Origin White Paper, José Barato, Juan Carlos Gracia, Ricard Manias, Alejandro Elíces, July 2004
5. Aljosa Pasic, Daniel Serrano, Pedro Soria, James Clarke, Pedro Carvalho, Antonio Maña: Security and Dependability in the Evolving Service-Centric Architectures, Published in the Book “At Your service”, MIT Press 2009
6. http://www.coso.org/
7. Marwane El Kharbili, Sebastian Stein, Ivan Markovic, Elke Pulvermüller, Towards a Framework for Semantic Business Process Compliance Management, , Proceedings of GRCIS 2008
8. Trent Henry, Products for Managing Governance, Risk, and Compliance: Market Fluff or Relevant Stuff?, Burton Group In-Depth Research Report Mar 18, 2008
9. Bitsaki, M., Danylevych, O., Van den Heuvel, W.J., Koutras, G., Leymann, F., Mancioppi, M., Nikolaou, C., Papazoglou, M.: An Architecture for Managing the Lifecycle of Business Goals for Partners in a Service Network. In: ServiceWave2008.
10. Bitsaki, M., Danylevych, O., Van den Heuvel, W.J., Koutras, G., Leymann, F., Mancioppi, M.,Nikolaou, C., Papazoglou, M.: Model Transformations to Leverage Service Networks. In: Proceedings of the 4th International Workshop on Engineering Service-Oriented Applications (WESOA 2008), Springer-Verlag (2008)

11. Namiri, K., Stojanovic., N.: Towards Business Level Verification of Cross-Organizational Business Processes. In Workshop on Semantics for Business Process Management (SBPM07), Budva, Montenegro, 2006
12. Namiri, K., Stojanovic., N.: A Formal Approach for Internal Controls Compliance in Business Processes. In 8th Workshop on Business Process Modeling, Development, and Support (BPMDS07), Trondheim, Norway, 2007.
13. Sadiq S., Governatori G., Namiri K.: Modeling Control Objectives for Business Process Compliance In Proceedings of the 5th International Conference, BPM 2007, Brisbane, Springer, 2007, pp.149-164.
14. M. E. Kharbili1, S. Stein, I. Markovic, and E. Pulvermuller. Towards a Framework for Semantic Business Process Compliance Management. In GRCIS 2008, June 2008
15. Tobias Anstett, Ganna Monakova, Daniel Schleicher, Steve Strauch, Ralph Mietzner, Dimka Karastoyanova, and Frank Leymann: MC-Cube: Mastering Customizable Compliance in the Cloud
16. Williamson Olivier, The Economic Institutions of Capitalism. New York: The Free Press, 1985
17. Aljosa Pasic, Pedro Soria-Rodriguez, Beatriz Gallego-Nicasio, Javier Calvo, Rafael Llarena, Charles Bastos, Towards a Real-Time Risk Assessment for Compliance Enforcement, eChallenges 2009, Istambul 21-23 October 2009
18. MASTER Technical Architecture, D2.3.2, available at http://www.master-fp7.eu/
19. Refsdal, A. and Stølen, K., Employing key indicators to provide a dynamic risk picture with a notion of confidence, Proceedings of the 3rd IFIP International Conference on Trust Management (IFIPTM'2009), 2009.
20. Manuel Gil Perez, Gabriel Lopez, Antonio F. Gomez Skarmeta, Aljosa Pasic, Advanced Policies for the Administrative Delegation in Federated Environments, submitted to DEPEND 2010 conference
21. Daniel Schleicher, Tobias Anstett, Frank Leymann, and Ralph Mietzner, Maintaining Compliance in Customizable Process Models
22. V. Di Giacomo, K. Julisch, S. Burri, G. Karjoth, T. Martin, P. Miseldine, N. Bielova, B. Crispo, F. Massacci, S. Neuhaus, N. Rassadko, A. Pretschner, and A. Refsdal. Protection and Assessment Model for Single Trust Domain. Public Deliverable of EU Research Project D2.1.1, MASTER - Managing Assurance, Security and Trust for sERvices, Report available at www.master-fp7.eu, 2009.
23. M. Blaze, J. Feigenbaum, J. Lacy. Decentralized Trust Management. IEEE Symposium on Security and Privacy. Oakland CA, 1996
24. M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized Trust Management. In Proc. 17th IEEE Symposium on Security and Privacy, pages 164–173. IEEE Computer Society Press, May 1996.
25. M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis. The KeyNote Trust-Management System, Version 2. IETF RFC 2704, September 1999.
26. D. Clarke, J.E. Elien, C. Ellison, M. Fredette, A. Morcos, and R. L. Rivest. Certificate Chain Discovery in SPKI/SDSI. Journal of Computer Security, 9(4):285–322, 2001.
27. M. Y. Becker and P. Sewell. Cassandra: Distributed Access Control Policies with Tunable Expressiveness. In Proc. 5th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2004), pages 159–168. IEEE Computer Society Press, 2004.
28. A. Herzberg, Y. Mass, J. Michaeli, Y. Ravid, and D. Naor. Access Control Meets Public Key Infrastructure, Or: Assigning Roles to Strangers. In Proc. IEEE Symposium on Security and Privacy, pages 2–14. IEEE Computer Society Press, 2000.
29. C. Gunter and T. Jim. Policy-directed Certificate Retrieval. Software: Practice & Experience, 30(15):1609–1640, September 2000.